UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [REDACTED EMAIL ADDRESS] THAT IS STORED AT PREMISES CONTROLLED BY [REDACTED SERVICE PROVIDER]

----------X

MEMORANDUM AND ORDER

16M1081

JAMES ORENSTEIN, Magistrate Judge:

The government has applied for a search warrant pursuant to the Stored Communications Act, 18 U.S.C. § 2701, *et seq.* (the "SCA"), that would require a provider of electronic communication service (the "Provider") to disclose to the government certain information, including the content of communications. *See* Affidavit in Support of an Application for a Search Warrant dated November 28, 2016 ("Affidavit"), at ¶¶ 1-2 (filed under seal); 18 U.S.C. § 2703(a), (b)(1)(A), (c)(1)(A). As explained in greater detail below, I conclude that the pertinent subscriber's knowledge of and consent to the requested disclosure renders a search warrant unavailable, and I therefore deny the application.

The affidavit submitted in support of the warrant application notes that "the user of the SUBJECT EMAIL ACCOUNT, [redacted name ("the Defendant")], has voluntarily consented, in the presence of [the Defendant's] counsel, to a search of the entire contents of the SUBJECT EMAIL ACCOUNT, without limitation, and [the Defendant] has not withdrawn [such] consent." Affidavit ¶ 3. Indeed, the Defendant has already been arrested, entered into a formal cooperation agreement with the government, pleaded guilty to an information charging the Defendant with the same offenses the government now seeks to investigate,[1] and been debriefed on multiple occasions by law enforcement agents. *Id.* ¶¶ 9-12. Of particular relevance here, the affiant reports:

---

[1] *Compare* Affidavit ¶ 7 (asserting that "there is probable cause to believe the SUBJECT EMAIL ACCOUNT will contain evidence, fruits and instrumentalities of violations of [redacted list of federal criminal offenses] (collectively, the 'Subject Offenses')"), *with id.* ¶ 11 ("On or about [redacted date], [the Defendant] pleaded guilty ... to an information charging the Subject Offenses.").

> [The Defendant] has stated, in sum and substance and in part, that [the Defendant] controlled and used the SUBJECT EMAIL ACCOUNT in furtherance of the Subject Offenses. [The Defendant] has also indicated that the SUBJECT EMAIL ACCOUNT will contain communications concerning [the Defendant's] involvement in the Subject Offenses. [The Defendant] has voluntarily consented, in the presence of [the Defendant's] counsel, to a search of the entire contents of the SUBJECT EMAIL ACCOUNT and [the Defendant] has not withdrawn [the Defendant's] consent to search the account. A request to preserve the SUBJECT EMAIL ACCOUNT, pursuant to 18 U.S.C. § 2703(f), has been served on [Provider].

Id. ¶ 12. After recounting that history, the affiant then concludes the proffer of facts establishing probable cause by noting that

> [b]ased on my knowledge, training and experience, I understand that it is preferable from an evidentiary and chain-of-custody standpoint to have an email service provider such as [Provider] to produce a true and correct copy of the contents of an email account, rather than log into the email account myself and search its contents.

Id. ¶ 13.[2]

The SCA provides a variety of methods for the government to secure different kinds of information from a provider of electronic communication service in the furtherance of a criminal investigation. Two are pertinent here:

> (b) Contents of wire or electronic communications in a remote computing service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
>
> > (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or
> >
> > (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

[2] The Affidavit does not specify whether the government has already sought to obtain the records at issue based on the Defendant's consent. I know from prior similar applications that some providers of electronic communication service decline to disclose comparable information without a warrant. As explained below, however, applicable law allows the government to require the Provider to disclose the non-content records upon the subscriber's consent, and also allows the government to secure the contents of the pertinent emails by means of a subpoena on notice to the subscriber.

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

18 U.S.C. § 2703(b).

(c) Records concerning electronic communication service or remote computing service.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

> (F) means and source of payment for such service (including any credit card or bank account number),
>
> of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

Id. § 2703(c)(1)-(2).

With respect to the government's request for a warrant compelling the disclosure of the contents of the Defendant's emails, the warrant procedure is inapposite. With respect to the request for other records pertaining to the Defendant's email account with the Provider, the warrant application is one available procedure, but the fact of the Defendant's consent to the disclosure renders it unnecessary, and thereby renders that portion of the application moot. I address each issue in turn below.

The Affidavit reveals that the Defendant has consented to allow the government to access the contents of the emails in the pertinent account, and therefore plainly has notice of the request. As a result, the pertinent provision of the SCA explicitly authorizes the government to secure the contents it seeks by means of a subpoena or a court order pursuant to subsection (d) of Section 2703. *Id.* § 2703(b)(1). The statute does not authorize using the Rule 41 warrant procedure in such circumstances; Congress has seen fit to provide for resort to the warrant procedure only in those circumstances in which the government seeks to proceed without notice to the subscriber. *Compare id.* § 2703(b)(1)(B), *with id.* § 2703(b)(1)(A). I assume that Congress understood what it was doing when it wrote the statute that way, and indeed such a structure makes sense: the distinction promotes judicial economy by imposing the burdens attendant to the warrant procedure (on both the executive and judicial branches) only in those instances in which it is necessary to preserve the secrecy of the government's investigation from the service subscriber whose communications the government seeks to access. No such necessity exists here; with the Defendant's consent, the government can secure the

information it wants in the form it prefers without resort to the warrant process simply by issuing a grand jury or trial subpoena. *See id.* § 2703(b)(1)(A).[3]

The government's request for a warrant compelling the disclosure of the Defendant's non-content account records is permissible under the SCA, notwithstanding the Defendant's consent to the disclosure of such records. The pertinent statutory provision allows for disclosure based on either. *See id.* § 2703(c)(1)(A), (C). The problem is not that issuing a warrant contravenes the statute; the problem is that doing so will do nothing to alter the legal rights and obligations of any person or entity. Because the government has secured the Defendant's consent, it already has the right to access the Defendant's account records – and the Provider has a corresponding legal obligation to disclose them. *Id.* § 2703(c)(1)(C). "'Federal courts are without power to decide questions that cannot affect the rights of litigants before them.'" *DeFunis v. Odegaard*, 416 U.S. 312, 316 (1974) (quoting *North Carolina v. Rice*, 404 U.S. 244, 246 (1971)); *Pitkin Supermarket, Inc. v. United States*, 2016 WL 6879254, at *4 (E.D.N.Y. Nov. 21, 2016) (quoting same); *see also Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) (holding that redressability is an element of the "irreducible constitutional minimum of standing"). Accordingly, deciding whether the government has established probable cause to believe that the Defendant's email account records will constitute evidence, fruits and instrumentalities of the Subject Offenses will not affect the government's right to compel the Provider to disclose those records. As a result, notwithstanding the SCA's applicability to a broad set of circumstances including those of this case, this court lacks the constitutional authority to determine the question of probable cause presented by the government's application.

---

[3] Because the government has asked only for a warrant pursuant to Section 2703(b)(1)(A), I need not and do not decide whether the Defendant's consent, and the availability of the evidence the government seeks by means of a subpoena, would moot any future request for a court order compelling the disclosure of the contents of the Defendant's emails pursuant to subsections (b)(1)(B) and (d) of the same section.

For the reasons set forth above, I deny the government's application for a warrant and an order of disclosure pursuant to the Stored Communications Act. Notwithstanding that denial, it is clear that the government has sufficient authority to take unilateral action, in the form of a subpoena for copies of email communications and a request for disclosure of other records based on the subscriber's consent, to compel the relevant service provider to disclose the evidence it seeks.

SO ORDERED.

Dated: Brooklyn, New York
November 28, 2016

/s/
JAMES ORENSTEIN
U.S. Magistrate Judge